STN Karlsruhe

```
=> s de19718284/PN
L4            1 DE19718284/PN
```

L4 ANSWER 1 OF 1 WPINDEX COPYRIGHT 2004 THOMSON DERWENT on STN

TI Monitoring system for safe operation of manufacturing plant with multiple modules, e.g robot handling system - has dual redundancy safety units built into each module and coupled to each other.

PI	EP 875810	A2	19981104	(199848)*	GE	10	G05B019-418
	R: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI						
	DE 19718284	A1	19981224	(199906)			G05B009-00 <--
	JP 10320003	A	19981204	(199908)		7	G05B009-03
	CN 1198375	A	19981111	(199913)			B25J013-00
	KR 98086661	A	19981205	(200009)			G05B019-418
	DE 19718284	C2	20010927	(200156)			G05B009-00 <--
	RU 2175451	C2	20011027	(200201)			G05B023-02
	US 2002052717	A1	20020502	(200234)			G06F011-00
	US 6385562	B1	20020507	(200235)			G06F011-00
	EP 875810	B1	20020814	(200255)	GE		G05B019-418
	R: DE FR GB IT SE SI						
	DE 59805151	G	20020919	(200264)			G05B019-418

AB EP 875810 A UPAB: 20021105

The manufacturing plant can be in the form of a robot handling system that has a power module [1] containing electrics and mechanical elements and this is coupled to a control module [2]. A hand held cycle programming unit [3] is coupled to the controller together with peripherals [4,5]

Each module has a safety unit [6.1- 6.5] based on dual microprocessors, RAM and ROM memory. Pairs of serial data lines [7,8] connect the safety units together.

ADVANTAGE - Provides distributed checks for high reliability identification of faults.

Dwg.1/3

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 197 18 284 C 2**

(51) Int. Cl.[7]:
G 05 B 9/00
F 16 P 3/00
B 25 J 17/00

(21) Aktenzeichen: 197 18 284.4-32
(22) Anmeldetag: 1. 5. 1997
(43) Offenlegungstag: 24. 12. 1998
(45) Veröffentlichungstag der Patenterteilung: 27. 9. 2001

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
KUKA Roboter GmbH, 86165 Augsburg, DE; IGM Robotersysteme AG, Wiener Neudorf, AT

(74) Vertreter:
Lichti und Kollegen, 76227 Karlsruhe

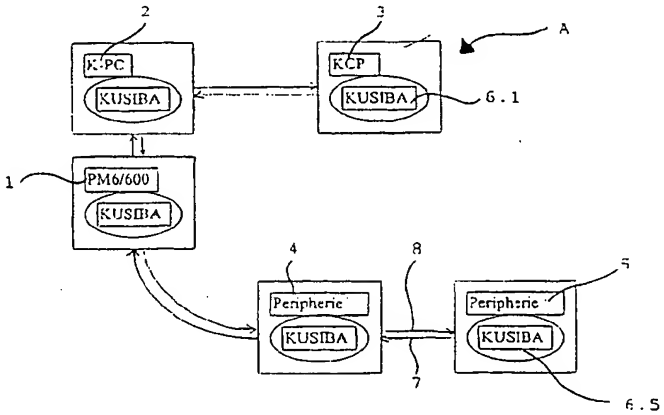
(72) Erfinder:
Roth, Stefan, 86485 Biberbach, DE; Schwarzinger, Wolfgang, Dr., Wien, AT

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 42 23 435 C2
DE 40 41 062 C2
DE 1 96 20 065 A1
DE 37 06 325 A1

(54) Verfahren und Vorrichtung zum Überwachen einer Anlage mit mehreren Funktionseinheiten

(57) Verfahren zum Überwachen einer Anlage mit mehreren Funktionseinheiten, wobei jede Funktionseinheit durch jeweils eine eigene zweikanalige und in sich redundante Sicherheitseinrichtung individuell überprüft wird, die beiden Kanäle jeder Sicherheitseinrichtung ständig verglichen werden, die Sicherheitseinrichtungen laufend einander über ihren Überprüfungszustand unterrichten und bei einer Fehlfunktion mindestens einer Funktionseinheit oder Sicherheitseinrichtung mindestens ein sicherheitsrelevantes Stellglied betätigt wird.



DE 197 18 284 C 2

DE 197 18 284 C 2

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum Überwachen einer Anlage mit mehreren Funktionseinheiten.

Bei einer Anlage, wie einer Fertigungsanlage, von der die Erfindung ausgeht, kann es sich um eine oder mehrere einander zugeordnete Maschinen handeln, wie beispielsweise Roboter. Eine Maschine bzw. ein Roboter besteht aus mehreren unterschiedlichen Funktionseinheiten, wie dem Leistungsteil (Power Modul), einer Steuereinheit und einer Bedienungseinheit. In einer Anlage, von der ausgegangen wird, können mehrere solche Maschinen mit den genannten Funktionseinheiten zusammenarbeiten und miteinander verknüpft sein. Weiterhin kann Peripherie vorhanden sein, wie Schienen, auf denen die Maschinen, wie Roboter, verfahren werden oder ein Portal, das die Maschinen oder Roboter entlang eines zu bearbeitenden "Werkstücks", wie eines Schiffes, verfährt.

Bisher werden bei Steuereinrichtungen parallele Not-Aus-Verdrahtungen vorgenommen, die in Relaistechnik verwirklicht werden. Probleme ergeben sich dabei mit der Sicherheit bei Programmierhandgeräten (Bedienungseinheiten), deren flexible Anschlußkabel vielen Einwirkungen ausgesetzt sind, so daß ein Kurzschluß zwischen Not-Aus-Leitungen nicht sicher ausgeschlossen werden kann. Die notwendige Zweikanaligkeit macht die Kabel zudem steif, dick und schwer. Parallel verdrahtete Sicherheitskreise sind applikationsspezifisch ausgelegt und bieten keine Flexibilität. Funktionelle Abweichungen sind nur durch eine Umkonstruktion möglich. Not-Aus-Schleifen und Bedienerschutz-Schleifen sind zwar erweiterbar, sie bieten aber nicht die Möglichkeit einer Diagnose, wenn ein Signalgeber im Sicherheitskreis einer Maschinensteuerung geöffnet ist. Darüber hinaus sind derartige Sicherheitseinrichtungen unübersichtlich und schwierig zu warten, wobei gerade die große Zahl der beteiligten Kontakte der Sicherheitslogik wiederum einen negativen Einfluß auf die Betriebssicherheit hat.

Die DE 37 06 325 A1 zeigt ein Steuer- und Datennetzwerk, bei dem eine Anzahl von Anschaltmodulen mit je einem Prozessor mit zugehörigen Bauteilen sowie wenigstens einer Eingangsschaltung und einer Ausgangsschaltung zur Aufnahme bzw. Abgabe von Daten und Signalen parallel an einen Bus angeschlossen ist. Die Anlage weist einen gemeinsamen Leitrechner auf, der die Anschaltmodule über den Bus mittels adressierter Telegramme aufruft und Daten- und Steuerinformationen überträgt sowie Antworten der Anschaltmodule aufnimmt. Nachteilig ist, daß ein zentraler Leitrechner vorhanden sein muss, der die Anschaltmodule mittels adressierbarer Telegramme aufruft und derart Daten- und Steuerinformationen überträgt sowie Antworten der Anschaltmodule aufnimmt. Dadurch, daß die einzelnen Module oder Knoten an der Adressierung von einem zentralen Rechner abhängig sind, ist das System relativ störanfällig.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zum Überwachen einer Anlage zu schaffen, die eine hohe Überwachungssicherheit aufweist.

Erfindungsgemäß wird die genannte Aufgabe durch ein Verfahren und eine Vorrichtung mit den Merkmalen der Ansprüche 1 bzw. 7 gelöst.

Die Erfindung sieht eine verteilte Sicherheitslogik vor, bei der jede Sicherheitseinrichtung sämtliche erforderlichen Sicherheitsfunktionen aufweist. Hierdurch ist eine hochauflösende Diagnose möglich. Die Sicherheitseinrichtungen stehen miteinander in Verbindung bzw. kommunizieren miteinander, so daß sie sich auch gegenseitig überwachen können und eine Sicherheitseinrichtung den Ausfall einer anderen erkennt und damit ein sicherheitsrelevantes Signal zur Betätigung eines Stellglieds ausgeben kann.

In einer ersten bevorzugten Ausgestaltung ist vorgesehen, daß die Sicherheitseinrichtungen eine Schnittstellenbeschaltung aufweisen. Hierdurch können die Sicherheitseinrichtungen sehr einfach und übersichtlich aufgebaut sein.

In bevorzugter Ausgestaltung ist dabei vorgesehen, daß die Sicherheitseinrichtungen seriell miteinander kommunizieren bzw. daß die Sicherheitseinrichtungen seriell miteinander verbunden sind. Durch die serielle Verbindung wird eine parallele Verdrahtung überflüssig. Notwendige Kabelquerschnitte können reduziert werden, was insbesondere für portable Geräte, wie Bedien- oder Programmierhandgeräte, äußerst vorteilhaft ist.

In weiterer bevorzugter Ausgestaltung ist vorgesehen, daß die Sicherheitseinrichtungen mittels eines Ringprotokolls miteinander kommunizieren bzw. daß die Sicherheitseinrichtungen in einem Ring miteinander verbunden sind. Damit ist die gesamte Sicherheitsvorrichtung in einfacher Weise beliebig erweiterbar. Wenn beispielsweise die Anlage weitere Funktionseinheiten erhält, so können die zugehörigen Sicherheitseinrichtungen ohne weiteres in einfacher Weise integriert werden. Es wird hierdurch eine einfache und übersichtliche Anpaßbarkeit an verschiedene Anlagen gewährleistet. Die Adressierung kann dabei physikalisch durch Plazierung im Bus erfolgen. Eine sichere Reaktion ist auch bei Erweiterung des Ringprotokolls sofort erreichbar.

Weitere bevorzugte Ausgestaltungen sehen vor, daß jede Sicherheitseinrichtung Diagnoseeingänge aufweist, wobei insbesondere die Diagnoseeingänge mit Prüf-Schaltzyklen der sicherheitsrelevanten Eingänge synchronisiert sind bzw. die Sicherheitseinrichtungen laufend eine Diagnose der ihnen zugeordneten Funktionseinheit und damit der Anlage durchführen. Hierdurch können Signalgeber, die ein sicherheitsrelevantes Signal abgegeben haben, lokalisiert werden. Darüber hinaus kann eine permanente Überwachung und Diagnose der gesamten Anlage vorgenommen werden.

In weiterer bevorzugter Ausgestaltung ist vorgesehen, daß in den Sicherheitseinrichtungen enthaltene Mikroprozessoren zyklisch ihr Prozessabbild und das daraus kalkulierte Ergebnis und/oder den Inhalt von Speichern überprüfen, wobei insbesondere der korrekte Anschluß und die Funktion von Signaleingängen und Signalgebern überprüft wird. Insbesondere bei einer redundanten Ausgestaltung der Sicherheitseinrichtungen in der oben skizzierten Weise können die Mikroprozessoren sich gegenseitig und die umgebende Hardware zyklisch abprüfen, wobei gleichzeitig das ablaufende Programm auf Konsistenz geprüft werden kann. Der Inhaltsvergleich der Prozessoren erfolgt dabei bei einem Ringprotokoll über den gesamten Ring.

Jede Sicherheitseinrichtung weist mindestens einen sicherheitsrelevanten Ausgang aufweist und/oder daß jede Sicherheitseinrichtung mehrere sicherheitsrelevante Eingänge aufweist.

Sowohl die gesamte Sicherheitsstruktur wird einfach und besonders preiswert, wenn in Weiterbildung vorgesehen ist, daß die Sicherheitseinrichtungen identisch zueinander ausgebildet sind, wobei vorzugsweise auch die in die identischen Sicherheitseinrichtungen integrierte Grundsoftware identisch ist und Anpassungen lediglich über Softbausteine oder -schalter erfolgen.

Das erfindungsgemäße Verfahren und die erfindungsgemäße Lösung weisen wesentliche Vorteile auf. Die Ringstruktur der gesamten Überwachungsvorrichtung ist erst geschlossen, wenn sich alle Funktionseinheiten und ihnen zugeordneten einzelnen Sicherheitseinrichtungen in Betrieb befinden. Die Kommunikation wird unterbrochen, wenn

eine Sicherheitseinrichtung eine Fehlfunktion zeigt; bei einer solchen andauernden Störung erfolgt eine Abschaltung und das Gesamtsystem tritt in einen sicheren Zustand.

Weitere Vorteile bestehen in der durch die Erfindung erreichten dezentralen Struktur, die, wie gesagt, flexibel erweiterbar ist und dennoch eine zuverlässige Betriebssicherheit bei geringem Platzbedarf und geringen Kosten erreicht. Durch die erfindungsgemäße Lösung wird der Verdrahtungsaufwand minimiert, Diagnosemöglichkeiten werden verbessert. Die Sicherheitseinrichtungen gemäß der Erfindung sind leicht in vorhandene Geräte zu integrieren.

Weitere Merkmale der Erfindung ergeben sich aus den Ansprüchen und aus der nachfolgenden Beschreibung, in der eine bevorzugte Ausführungsform der Erfindung unter Bezugnahme auf die Zeichnung im einzelnen erläutert ist.

Dabei zeigt:

Fig. 1 einen schematischen Aufbau einer erfindungsgemäßen Vorrichtung an einer zu überwachenden Anlage;

Fig. 2 eine schematische Darstellung einer Sicherheitseinrichtung der erfindungsgemäßen Vorrichtung; und

Fig. 3 ein Diagramm der durch die Erfindung gewährleisteten Betriebszustände der erfindungsgemäßen Vorrichtung.

Eine erfindungsgemäße Vorrichtung dient zur Überwachung einer Anlage A, wie einer Fertigungsanlage; eine solche weist beispielsweise eine Leistungseinheit **1** auf, die die Leistungselektronik und die mechanischen Elemente einer Maschine oder eines Roboters beinhalten. Der Leistungseinheit **1** ist eine Steuereinheit zugeordnet, die die Signalelektronik zur Steuerung der Leistungseinheit **1** enthält und als reine Hardwareschaltung oder in gewünschter Abstufung mit Softwareelementen, bis hin zu einer reinen Computersteuerung, ausgebildet sein kann. Bei einem Roboter sind heute Leistungseinheit **1** und Steuereinheit **2** in der Regel körperlich und räumlich getrennt ausgelegt. Eine Anlage, von der die Erfindung ausgeht, kann weiterhin eine Bedieneinheit **3** aufweisen, die beispielsweise ein Programmierhandgerät sein kann, das im konkreten Fall zum Programmieren eines Roboters, wie der Steuereinheit **2**, dienen kann und in einem solchen Fall ebenfalls räumlich und körperlich getrennt von diesem ausgebildet ist.

Weiterhin kann eine derartige Anlage Peripherien **4**, **5** aufweisen, wie beispielsweise eine Verfahreinrichtung für die Leistungseinheit **1** oder aber beispielsweise im Schiffsbau ein Portal, auf dem mehrere Leistungseinheiten **1** angeordnet sind.

Die Erfindung sieht nun vor, daß jeder der Funktionseinheiten **1** bis **5** eine separate Sicherheitseinrichtung **6.1–6.5** zugeordnet ist. Die Sicherheitseinrichtungen 6.1– 6.5 sind vorteilhafterweise identisch ausgebildet und daher in der **Fig.** 2 lediglich mit dem Bezugszeichen **6** versehen. Eine Sicherheitseinrichtung **6** weist (mindestens) zwei Microcontroller auf. Diese haben ausreichend integrierte RAMs oder ROMs sowie mindestens einen seriellen Anschluß. So kann die Zweikanaligkeit der Sicherheitskreise bis in die Auswertung hinein aufrecht erhalten werden. Die zwei Kanäle des redundanten Systems werden ständig verglichen. Je nach Verwendung ist eine unterschiedliche Schnittstellenbeschaltung vorgesehen. Die Sicherheitseinrichtungen **6.1–6.5** stehen über ankommende und weiterleitende Schnittstellen bzw. Leitungen **7**, **8** miteinander in Verbindung. Die Verbindung ist vorzugsweise weiterhin in einer Ringstruktur mit Hin- und Rückleitungen **7**, **8** ausgebildet.

Eine erfindungsgemäße Sicherheitseinrichtung **6** weist neben den seriellen Anschlüssen oder Leitungen **7**, **8** zur Verbindung mit den anderen Sicherheitseinrichtungen sicherheitsrelevante Eingänge **10–14** auf, die mit der jeweiligen Funktionseinheit und einzelnen Bedienungselementen derselben verbunden sind und zum Einlesen sicherheitsrelevanter Signale dienen. Sicherheitsrelevante Eingänge leiten entweder einen Stop unbedingt ein oder sind Bedingung für einen solchen Stop. Die Eingänge **11–14** sind doppelt ausgeführt, so daß jeder Mikrocontroller über einen unabhängigen Eingang mit identischer Funktion verfügt. Weiter können Eingänge ohne Sicherheitsfunktion vorgesehen sein. Diese werden auch als Diagnoseeingänge bezeichnet und haben auf beiden Mikrocontrollern unterschiedliche Bedeutung. Alle sicherheitsrelevanten Eingänge **11–14** werden durch beide Mikrocontroller parallel ausgewertet. So kann ein Eingang mit einer Zustimmungstaste, ein anderer mit einer Not-Aus-Taste und ein weiterer mit einer Wahltaste für Test- oder Automatikbetrieb verbunden sein. Darüber hinaus ist ein Eingang zum Anschluß weiterer Bedienerschutz-Einrichtungen vorgesehen. Nicht sämtliche Eingänge müssen in jeder Funktionseinheit belegt sein. So werden die vorstehend erstgenannten Eingänge insbesondere bei der Bedieneinheit belegt sein, während der letztgenannte Eingang (Bedienerschutz) bei der Leistungseinheit bzw. auch einzelnen Peripherieeinheiten belegt ist.

Im einzelnen gilt:

Lokaler Not-Aus = LNA

Dies ist der Eingang für den lokale Not-Aus, der durch Betätigen des Roboters NOT-AUS an der Bedienungseinheit oder durch eine andere Not-Aus-Bedingung ausgelöst wird. Er führt unter allen Umständen zum Stillsetzen und Energiefreischalten des Roboters sowie der gesamten Anlage, in die der Roboter integriert ist.

Externe Not-Aus-Anforderung = eNAA

Dieser Eingang führt unter allen Umständen zum Abschalten des Roboters. Die Not-Aus-Anforderung wird in diesem Fall nicht an die Anlage weitergegeben, da dies zum Verriegeln derselben führen würde.

Bedienerschutz = BS

Der Bedienerschutz-Eingang setzt nur die Sicherheitszelle selbst still. Unter Sicherheitszelle wird hier der Bereich verstanden, der von einer Kinematik gefahrbringend durchfahren werden kann. Bei einer Roboterzelle ist dies z. B. der durch Schutzzäune begrenzte Arbeitsbereich des Roboters selbst sowie der Zusatzachsen, die gefährdende Bewegungen ausführen können.

Der Bedienerschutz ist aktiv, wenn die Steuerung in der Betriebsart Automatik arbeitet. Das anstehende Bedienerschutzsignal ist gleichbedeutend mit dem geschlossenen Schutzzaun der Sicherheitszelle.

1. Qualifizierter Eingang **1** (Test/Auto) = QE1

Der Eingang **13** für Test/Automatik ist ein qualifizierendes Signal. In der Betriebsart Test ist der Bedienerschutz abgeschaltet und dafür die Zustimmtasten aktiv. In der Betriebsart Automatik ist der Bedienerschutz aktiv, die Zustimmtasten werden dabei nicht abgefragt. Die Sicherheitszelle kann sich entweder in der Test- oder in der Automatik-Betriebsart befinden. Beide Betriebsarten gleichzeitig sind genauso wenig möglich wie keine Betriebsart. Das Ruhestromprinzip ist hier nur schwer einzuhalten, weil beide Einstellungen aktive Einstellungen sind. Es ist deshalb sinnvoll, gegenparallele Pegel zu verwenden. Es ergibt sich, daß das Signal bei den Microcontrollern einmal als Automatik und einmal als Nicht-Automatik eingelesen wird. Im

folgenden wird anstelle der Bezeichnung/Automatik die Bezeichnung Test verwendet.

2. Qualifizierender Eingang 2 = QE2

Für den Eingang **14** gilt die gleiche Maßgabe wie für Eingang **13**. Dieser Eingang **14** wird für Steuerungen benötigt, die eine Überbrückung des Bedienerschutzes in der Betriebsart Test benötigen. Bei Überbrückung der Schutzeinrichtung in der Betriebsart Automatik wird, wie bei einer Verletzung des Bedienerschutzes die Zelle stillgesetzt.

Es sind weiterhin Ausgänge **15**, **16** vorgesehen, die, soweit belegt, sicherheitsrelevante Stellglieder ansteuern und so zur Stillsetzung der Anlage bzw. zum Verfahren derselben in einen sicheren Zustand dienen. Informelle Eingänge **17** sind einkanalig ausgeführt. Das gesamte Sicherheitsnetz soll auch mit externer Spannung zu versorgen sein. Daraus ergibt sich, daß jede Sicherheitseinrichtung **6** eine Spannungsversorgung benötigt. Zu diesem Zweck wird mit der Kommunikationsleitung eine Spannungsversorgung verlegt. Die Nennspannung dieser Spannungsversorgung beträgt 24 V. Jeder Kern verfügt über eine eigene Erzeugung der Logikspannung.

Auch hier gilt im einzelnen:

Sicherheitsrelevante Ausgänge

Sicherheitsrelevante Ausgänge sind solche, deren ordnungsgemäße Funktion zum Abschalten der Anlagenenergie zwingend erforderlich ist.

Antriebe Ein = AE

Zu den sicherheitsrelevanten Ausgängen zählt die Ansteuerung für den Netzschutz der Antriebe durch das Antriebe Ein Signal. Dieser Ausgang ist an jeder Sicherheitseinrichtung vorhanden und ist sicher.

Not-Aus = NA

Der Not-Aus-Ausgang hat die Aufgabe, eine lokale Not-Aus-Anforderung in die Notausschleife einer kompletten Anlage einzuschleifen. Um potentialfreie Kontakte zu erhalten, wird der Knoten mit einer sicheren Relaiskombination ausgestattet.

Bedienerschutz = BS

Unter Bedienerschutz versteht man Einrichtungen zum Schutz des Bedieners. Dazu zählen Schutzzäune, deren Überwachungen und abhängig von der Betriebsart auch der Zustimmungsschalter. Im Knoten werden sämtliche Ausgänge solcher Einrichtungen zusammengefaßt. Der Bedienerschutz-Ausgang hat die Aufgabe, eine Verletzung des Bediener-Schutzes auch für beteiligte Anlagenteile wirksam zu machen. Um potentialfreie Kontakte zu erhalten, kann an den Knoten eine sichere Relaiskombination angeschlossen werden.

Weiter sind informelle oder Steuereingänge und informelle Ausgänge vorgesehen:

Informelle Eingänge

Informelle oder Steuereingänge **17** sind diejenigen, die zum ordnungsgemäßen Betrieb des Roboters notwendig sind. Diese Eingänge sind nicht sicherheitsrelevant und können frei verwendet werden. Sie stellen lediglich Informationen für Diagnosezwecke zur Verfügung. Die informellen Eingänge **17** sind synchronisiert mit den Prüf-Schaltzyklen der sicherheitsrelevanten Signale. So können auch verkettete Not-Aus-Taster zwischen den Kontakten eingelesen werden.

Antriebe Aktivieren = AA

Das Signal "Antriebe Aktivieren" ist ein Impuls, der die Antriebe einschalten soll, solange keine Sicherheitsanforderung dagegen spricht. Dieses Signal darf nicht dauernd aktiv gehalten werden.

Antriebe Freigabe = AF

Das "Antriebe Freigabe"-Signal hat die Aufgabe, die Antriebe durch Wegnahme abzuschalten bzw. ein Einschalten zu verhindern.

Not-Aus Info = NAi/Bedienerschutz Info = Bsi

Eine lokale Not-Aus- oder Bedienerschutz-Schleife kann mit diesen Eingängen zwischen den Kontakten abgegriffen werden, um bei einer Unterbrechung Informationen über den Ort der Sicherheitsanforderung zu erhalten.

Informelle Ausgänge

Informelle Ausgänge sind diejenigen, die ausgegeben werden, um den Status des Sicherheitsnetzwerks darzustellen. Informelle Ausgänge können zu einer Registerschnittstelle zusammengefaßt werden. Bei Anschluß eines Steuerungsrechners, in dem keine sicherheitsrelevanten Stellglieder vorhanden sind, können auch sicherheitsrelevante Ausgänge zu Informationszwecken verwendet werden.

I Not-Aus = iNA

Die Not-Aus-Information hat die Aufgabe, eine lokale Not-Aus-Anforderung an eine Steuerung oder Signalleuchte zu melden. Dieses Signal ist eine ODER-Verknüpfung aller Not-Aus-Bedingungen mit Ausnahme des Signals: externe NOT-AUS Anforderung.

I Fehler intern = iFi

Das Fehlersignal gibt Auskunft, ob es innerhalb der erfindungsgemäßen Vorrichtung zu einem Fehler gekommen ist, der zur Abschaltung geführt hat.

Im Leistungsteil **1** wird ein Ausgang **15** der Sicherheitseinrichtung **6** als Ausgang "Antriebe ein" zum Ansteuern eines Netzschützes verwendet. Es gibt ebenso die Möglichkeit, bei entsprechenden Fehlerzuständen direkt einen Not-Aus auszulösen.

Einer Sicherheitseinrichtung in der Steuereinheit **2** stehen alle Informationen und Zustände des Sicherheitskreises der Steuerungssoftware zur Verfügung. Auch hier wird ein Ausgang mit einem Not-Aus belegt sein, um einen solchen in der Steuereinheit **2** auszulösen.

Die Sicherheitseinrichtung **6.1** in einer Bedieneinheit **3** ist hauptsächlich Träger von Signalgebern für Not-Aus, Betriebsartenwahl und Ein- und Ausschalten der Antriebe. Eine Anzeige kann über Steuerungssoftware und ein Display erfolgen.

Sicherheitseinrichtungen **6.4** und **6.5** in der Peripherie **4**. **5** können Antriebsenergien für in einen Schutzkreis integrierte Servoschalter betätigen sowie Signalgeber wie Lichtvorhänge und zusätzlichen Not-Aus-Taster ausgedehnter Kinematiken in den Schutzkreis einbinden. Zum Zwecke

der Anzeige kann eine identische Sicherheitseinrichtung auch in entsprechende Bedientafeln integriert werden.

In der **Fig.** 3 sind schematisch die Betriebszustände der erfindungsgemäßen Sicherheitseinrichtungen dargestellt.

Der Bedienerschutz kann geöffnet oder geschlossen sein. Es kann eine Zustimm-Taste betätigt (Ja) oder nicht betätigt (Nein) sein. Es kann ein Automatik- oder Testbetrieb gewählt sein. Bei Automatikbetrieb ist, wie sich aus der Aufstellung ergibt, ein Betrieb nur möglich, wenn der Bedienerschutz geschlossen ist. Bei Wahl "Test" ist, ein Betrieb bei geöffnetem und geschlossenem Bedienerschutz möglich, aber nur, wenn gleichzeitig die Zustimm-Taste betätigt wird.

Die Betriebszustände können hinsichtlich weiterer Eingänge je nach Einsatz- bzw. Anwendungszweck erweitert werden.

In den Sicherheitseinrichtungen **6**, **6.1–6.5** erfolgt zunächst ein Vergleich der lokalen Ergebnisse der beiden Mikrocontroller und eine Überprüfung auf Abweichung. Ist ein Unterschied vorhanden, wird die Variable "Vergleich fehlgeschlagen" (Vf) inkrementiert. Sie gibt die Anzahl der Kommunikationszyklen an, bei denen nacheinander die Ergebnisse beider Kanäle nicht übereingestimmt haben. Sind die Ergebnisse konsistent, wird Vf zurückgesetzt oder dekrementiert. Wird die zwischen den beiden Kanälen maximal zulässige Kanalverzögerungszeit, die definiert ist durch Vf-max, überschritten, so wird "Not-Aus" ausgelöst und das Netzwerk verriegelt sich.

Der Informationskanal, der für den Vergleich genutzt wird, ist der gleiche serielle Kanal, der auch für die Kommunikation zwischen den Sicherheitseinrichtungen verwendet wird.

Ein Vergleich erfolgt während der laufenden Prozesskommunikation: Ein Schritt entspricht dem Datenumfang eines Mikrocontrollers. Ein Schiebeschritt, es ist abhängig von der Position des Mikrocontrollers der Sicherheitseinrichtung der erste oder der letzte pro Kommunikation, ist für den Vergleich vorgesehen. In diesem Schritt wird das Eingangs- und das Ausgangs-Abbild mit dem des parallelen Mikrocontrollers in der gleichen Sicherheitseinrichtung verglichen.

Ein weiterer Vergleich erfolgt bei Kommunikations-Beginn oder bei einer Zwischenkommunikation. Es wird dabei geprüft, ob der Vergleich der Prozessabbilder sowie das Führen des Vf nicht auch in der nächsten Sicherheitseinrichtung stattfinden kann. So kann ein Vergleich, bei dem eine Art Zwischenkommunikation erfolgt, nur zwei Schiebeschritte dauern. Im ersten Schritt überträgt jeder Mikrocontroller eigene Prozessdaten. Der jeweils zweite Mikrocontroller einer Sicherheitseinrichtung kann jetzt bereits vergleichen. Der jeweils erste Mikrocontroller merkt sich zunächst das Prozessabbild des vorigen Mikrocontrollers. Er führt den Vergleich nach dem zweiten Schiebeschritt durch. Der Vf-Zähler dieses Mikrocontrollers gilt also für den im Sicherheits-Kreis vorher angeordneten Sicherheitskern.

Im weiteren erfolgt eine Verknüpfung als eigentliche Funktion des Schierheitskreises: Zum einen wird aus den Eingängen jeder einzelnen Sicherheitseinrichtung ein eigenes Ergebnis gebildet: zum anderen werden die Ergebnisse der anderen Sicherheitseinrichtungen vor der Aktualisierung im lokalen Ergebnis berücksichtigt. Es gibt, zwei Möglichkeiten, die Ausgabe-Ergebnisse zu ermitteln: Es kann bei der Kommunikation das gesamte Prozeßabbild ausgetauscht werden und somit in jeder der Gesamt-Not-Aus parallel, aber in unterschiedlicher Reihenfolge verknüpft werden. Es kann ein Ausführungsbefehl gesendet werden. In diesem Befehl verknüpfen alle Sicherheitseinrichtungen ihre Ergebnisse, und es werden alle Ausgänge nach diesem Befehl geschaltet.

Man unterscheidet verschiedene Arten der sicheren Stillsetzung:

Die Funktion Not-Aus kann von verschiedenen Signalgebern ausgelöst werden. Alle angeschlossenen Signalgeber sind dabei zweikanalig angeschlossen. Beim Lösen der Not-Aus-Verriegelung kann eine unendliche Gleichzeitigkeit zwischen den Kanälen akzeptiert werden.

Der Not-Aus hat in unterschiedlichen Betriebsarten unterschiedliche Reaktionen zur Folge.

Im Automatikbetrieb ist dabei die Abschaltung des Netzes verzögert und sicher. Der eingeleitete Not-Aus wird von der Steuerung erkannt und es wird sofort eine Not-Aus-Stop-Rampe gefahren. Mit dieser Stop-Rampe bleibt der Roboter auf der programmierten Bahn. Der Roboter kommt in einem kalkulierten Punkt zum Stillstand.

Im Testbetrieb wird die Energieversorgung bei Not-Aus-Anforderung sofort abgeschaltet. Die Freigaben für die Antriebe bleiben, solange kein Antriebsfehler aufgetreten ist, aktiv. So wird gewährleistet, daß der Roboter mit dem kürzestmöglichen Bremsweg und damit am schnellsten in den sicheren Zustand gebracht werden kann.

Der Bedienerschutz versetzt nun die lokale Anlage in den sicheren Zustand. Der Bedienerschutz muß in den unterschiedlichen Betriebsarten mit veschiedenen Signalen verknüpft werden:

BS-Freigabe = Schutzgitter geschlossen & Automatik + Zustimmung gedrückt & Testbetrieb.

Der Bedienerschutz wirkt immer unverzögert auf die Energieabschaltung via Hauptschütz. Die Abschaltreaktion der Maschine oder des Roboters ist so zu gestalten, daß immer kürzeste Bremswege erreicht werden.

Die Kommunikation zwischen den Sicherheitseinrichtungen erfolgt seriell und geht durch beide Mikrocontroller hindurch, so daß jeder Mikrocontroller in der Lage ist, dem jeweils anderen über den Kommunikationsring das Prozessabbild zum Vergleich zur Verfügung zu stellen. Die Kommunikation dient zum Vergleich der Kanäle bei zweikanaligen Eingängen und zur deterministischen Aktualisierung des Ausgangsabbilds auf dem gesamten Bus. Jede Kommunikation erfolgt in Schiebeschritten. Ein Schritt entspricht dem Datenumfang eines Mikrocontrollers. Ein Schiebeschritt, es ist der erste oder der letzte pro Kommunikation, ist für den Vergleich vorgesehen. Alle anderen Schiebeschritte werden dazu benutzt, das Gesamtprozessabbild des Netzwerks in der einzelnen Sicherheitseinrichtung zu ermitteln. Dabei werden nur Prozessabbilder von anderen übernommen, welche von deren beiden Mikrocontrollern gleich übertragen wurden.

Patentansprüche

1. Verfahren zum Überwachen einer Anlage mit mehreren Funktionseinheiten, wobei jede Funktionseinheit durch jeweils eine eigene zweikanalige und in sich redundante Sicherheitseinrichtung individuell überprüft wird, die beiden Kanäle jeder Sicherheitseinrichtung ständig verglichen werden, die Sicherheitseinrichtungen laufend einander über ihren Überprüfungszustand unterrichten und bei einer Fehlfunktion mindestens einer Funktionseinheit oder Sicherheitseinrichtung mindestens ein sicherheitsrelevantes Stellglied betätigt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Sicherheitseinrichtungen seriell miteinander kommunizieren.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Sicherheitseinrichtungen mittels ei-

nes Ringprotokolls miteinander kommunizieren.

4. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß jede Sicherheitseinrichtung laufend eine Diagnose der ihr zugeordneten Funktionseinheit und unter Heranziehung der ihr von den anderen Sicherheitseinrichtungen übermittelten Informationen der gesamten Anlage durchführt.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß in den Sicherheitseinrichtungen enthaltene Mikroprozessoren zyklisch ihr Prozessabbild und das daraus kalkulierte Ergebnis und/oder den Inhalt von Speichern überprüfen.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß in den Sicherheitseinrichtungen der korrekte elektromechanische Anschluß und die Funktion von Signaleingängen und Signalgebern überprüft wird.

7. Vorrichtung zum Überwachen einer Anlage (A) mit mehreren Funktionseinheiten (**1** bis **5**), wobei jeder Funktionseinheit (**1** bis **5**) jeweils eine eigene zweikanalige und in sich redundante Sicherheitseinrichtung (**6**; **6.1** bis **6.5**) mit zwei einander vergleichenden Prozessoren zur individuellen Überprüfung der jeweiligen Funktionseinheit (**1** bis **5**) zugeordnet ist und die Sicherheitseinrichtungen (**6**; **6.1** bis **6.5**) derart miteinander verbunden sind, daß sie bei einer Fehlfunktion mindestens einer Funktionseinheit (**1** bis **5**) oder Sicherheitseinrichtung (**6**; **6.1** bis **6.5**) mindestens ein sicherheitsrelevantes Stellglied betätigen.

8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, daß die Sicherheitseinrichtungen (**6**; **6.1** bis **6.5**) eine Schnittstellenbeschaltung aufweisen.

9. Vorrichtung nach Anspruch 7 oder 8, dadurch gekennzeichnet, daß die Sicherheitseinrichtungen (**6**; **6.1** bis **6.5**) seriell miteinander verbunden sind.

10. Vorrichtung nach einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, daß die Sicherheitseinrichtungen (**6**; **6.1** bis **6.5**) in einem Ring miteinander verbunden sind.

11. Vorrichtung nach einem der Ansprüche 7 bis 10, dadurch gekennzeichnet, daß jede Sicherheitseinrichtung mindestens einen sicherheitsrelevanten Ausgang (**15**, **16**) aufweist.

12. Vorrichtung nach einem der Ansprüche 7 bis 11, dadurch gekennzeichnet, daß jede Sicherheitseinrichtung mehrere sicherheitsrelevante Eingänge (**11** bis **14**) aufweist.

13. Vorrichtung nach einem der Ansprüche 7 bis 12, dadurch gekennzeichnet, daß jede Sicherheitseinrichtung (**6**; **6.1** bis **6.5**) Diagnoseeingänge (**17**) aufweist.

14. Vorrichtung nach Anspruch 12 mit 13, dadurch gekennzeichnet, daß die Diagnoseeingänge (**17**) mit Prüf-Schaltzyklen der sicherheitsrelevanten Eingänge (**11** bis **14**) synchronisiert sind.

15. Vorrichtung nach einem der Ansprüche 7 bis 14, dadurch gekennzeichnet, daß die Sicherheitseinrichtungen (**6**; **6.1** bis **6.5**) identisch zueinander ausgebildet sind.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 197 18 284 C2
Int. Cl.[7]: G 05 B 9/00
Veröffentlichungstag: 27. September 2001

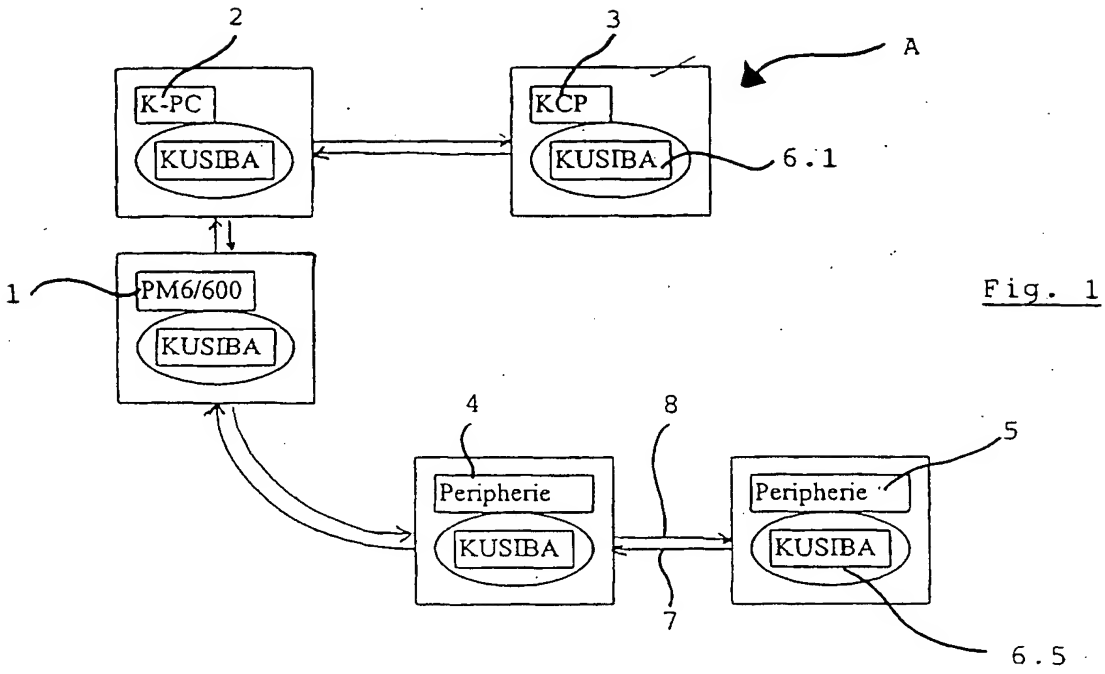


Fig. 1

Nummer: DE 197 18 284 C2
Int. Cl.[7]: G 05 B 9/00
Veröffentlichungstag: 27. September 2001

Bedienerschutz	geöffnet		geschlossen	
Zustimmung	nein	ja	nein	ja
Test (ja)	AUS	EIN	AUS	EIN
Automatik (ja)	AUS	AUS	EIN	EIN

Fig. 3

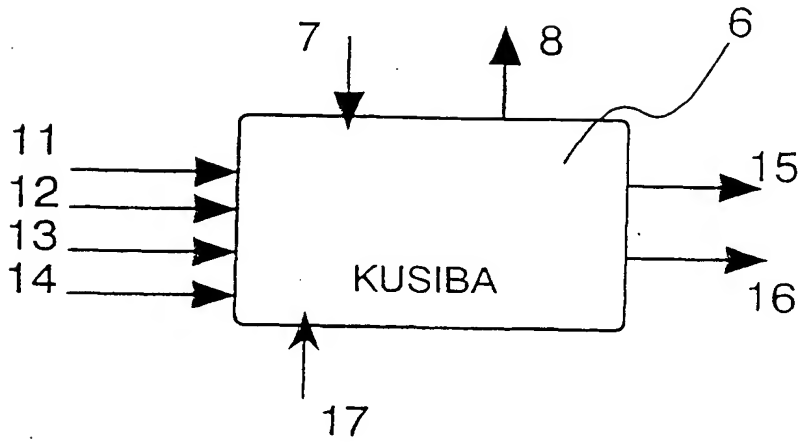


Fig. 2